Step 1: Install OSSEC Dependencies

OSSEC requires PHP, gcc, libc and Apache Web Server. Install them by running the commands below:

```
sudo apt install -y wget unzip make gcc build-essential

sudo apt install -y php php-cli php-common libapache2-mod-php apache2-utils sendmail inotify-tools
```

Step 2: Install OSSEC HIDS on Ubuntu 16.04

Once the dependencies have been installed, the next installation is for OSSEC HIDS. The source code for OSSEC is available on Github.

Check for the latest release before downloading. As of this writing, the latest is 3.1.0

```
export VER="3.1.0"

wget https://github.com/ossec/ossec-hids/archive/${VER}.tar.gz
```

Once downloaded, extract the file with the following command:

```
tar -xvzf ${VER}.tar.gz
```

This extraction will create a folder, change to this folder and run the install script.

```
cd ossec-hids-${VER}

sudo sh install.sh
```

A) OSSEC-HIDS SERVER SETTING

1. Set language

```
(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: en
```

2. Press <ENTER> to continue

```
OSSEC HIDS v3.1.0 Installation Script - http://www.ossec.net


 You are about to start the installation process of the OSSEC HIDS.

 You must have a C compiler pre-installed in your system.


  - System: Linux deb9 4.9.0-8-amd64

  - User: root

  - Host: deb9


  -- Press ENTER to continue or Ctrl-C to abort. --
```

3. Choose local installation type

```
1- What kind of installation do you want (server, agent, local or help)?
        - Server installation chosen.
2- Setting up the installation environment.
        - Choose where to install the OSSEC HIDS [/var/ossec]: /var/ossec
        - Installation will be made at /var/ossec
```

4.Configure alert notifications (this is what you will see on the screen):

- Configuring the OSSEC HIDS.
    - Do you want e-mail notifi cation? (y/n) [y]: y
    - What's your e-mail address? root@localhost ## use your sfsu email
    - We found your SMTP server as: 127.0.0.1 ## do not use local IP

    - Do you want to use it? (y/n) [y]: y
    --— Using SMTP server: 127.0.0.1 ## do not use local IP

5. Configure active response. A tool that takes automated actions to prevent intrusion or reduce the extent of an intrusion.

- Active response allows you to execute a specific command based on the events received. For example, you can block an IP address or disable access for a specific user. More information at: http://www.ossec.net/en/manual.html#active-response
- Do you want to enable active response? (y/n) [y]: y
- Active response enabled.
- By default, we can enable the host-deny and the firewall-drop responses. The fi rst one will add a host to the /etc/hosts.deny and the second one will block the host on iptables (if linux) or on
  ipfilter (if Solaris, FreeBSD or NetBSD).
- They can be used to stop SSHD brute force scans, portscans and some other forms of attacks. You can also add them to block on snort events, for example.
- Do you want to enable the firewall-drop response? (y/n) [y]: y
- Firewall-drop enabled (local) for levels >= 6
- Default white list for the active response:
  - 192.168.65.2
- Do you want to add more IPs to the white list? (y/n)? [n]: n

6. With a server installation, the OSSEC HIDS can receive alerts through an encrypted channel (port 1514) or through syslog (port 514).

    - Do you want to enable remote syslog (port 514 udp)? (y/n) [y]: y
    - Remote syslog enabled.
    - Setting the configuration to analyze the following logs:
    -- /var/log/messages
    -- /var/log/auth.log
    -- /var/log/syslog
    -- /var/log/mail.info
    - If you want to monitor any other file, just change
    the ossec.conf and add a new localfile entry.
    Any questions about the configuration can be answered
    by visiting us online at http://www.ossec.net .
    --— Press ENTER to continue —--

After you press Enter, the OSSEC HIDS is compiled, installed, and configured with the options you specified. When the installation is complete, the installer script provides you with some final information by sent a mail to you.

Start your OSSEC server use this: /var/ossec/bin/ossec-control start

B) OSSEC-HIDS CLIENT SETTING

Next, config ossec client web, You open backend server have web site(host-base). You must complete step 1 and download, run scrip on step2. After follow:

1. Set language

```
(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: en
```

2. Press <ENTER> to continue

```
OSSEC HIDS v3.1.0 Installation Script - http://www.ossec.net

 You are about to start the installation process of the OSSEC HIDS.

 You must have a C compiler pre-installed in your system.

 - System: Linux deb9 4.9.0-8-amd64

 - User: root

 - Host: deb9

 -- Press ENTER to continue or Ctrl-C to abort. --
```

3. Choose local installation type

```
1- What kind of installation do you want (server, agent, local or help)?
        - Agent installation chosen.
2- Setting up the installation environment.
        - Choose where to install the OSSEC HIDS [/var/ossec]: /opt/ossec

        - Installation will be made at /opt/ossec

Configuring the OSSEC HIDS.
 - What's the IP Address of the OSSEC HIDS server?: ip ossec server
 - Adding Server IP : ip ossec server
Do you want to run the integrity check daemon? (y/n) [y]: y
 - Running syscheck (integrity check daemon).
 Do you want to run the rootkit detection engine? (y/n) [y]: y
 Running rootcheck (rootkit detection).
```

4.Enable active response..

```
- - Do you want to enable active response? (y/n) [y]: y
        -- Setting the confi guration to analyze the following logs:
        -- /var/log/messages
        -- /var/log/authlog
        -- /var/log/secure
        -- /var/log/xferlog
        -- /var/log/maillog
        - If you want to monitor any other fi le, just change
        the ossec.conf and add a new localfi le entry.
        Any questions about the confi guration can be answered
        by visiting us online at http://www.ossec.net .
        --— Press ENTER to continue —--Start your OSSEC server
```

Step3: Adding agents to the server: (EXAMPLE)

1. Add the agent to the server (run the “manage_agents” command, provide the IP Address of the agent and choose a name for it or username).

```
(server)# /var/ossec/bin/manage_agents

****************************************
* OSSEC HIDS v0.8 Agent manager. *
* The following options are available: *
****************************************
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your actions: A,E,R or Q: a

- Adding a new agent (use ‘q’ to return to main menu).
Please provide the following:
* A name for the new agent: web
* The IP Address for the new agent: ip web agent

* An ID for the new agent[001]:
Agent information:
ID:001
Name:web
IP Address: ip web agent

Confirm adding it?(y/n): y
Added.
```

2. After agent is added, extract the authentication key from your server. In the “manage_agents”, choose the “E” option and provide the ID of the agent. The key to be used by the agent will be printed. Then, copy and paste it in the agent side.

```
(server)# /var/ossec/bin/manage_agents

****************************************
* OSSEC HIDS v0.8 Agent manager. *
* The following options are available: *
****************************************
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your actions: A,E,R or Q: e
```

```
Available agents:
ID: 001, Name: web, IP: ip web agent
Provide the ID of the agent you want to extract the key: 001

Agent key information for '001' is:
CDAxIGxpbnX4MSAxOTIuMTY4LjAuMzIgOWM5MENlYzNXXXYYYZZZZZ==

** Press ENTER to continue
```

3. After a key is generated, copy it and paste it on the agent side. Run the same "manage_agents" command in the agent.

```
(agent)# /var/ossec/bin/manage_agents

****************************************
* OSSEC HIDS v0.8 Agent manager. *
* The following options are available: *
****************************************
(I)mport key for the server (I).
(Q)uit.
Choose your actions: I or Q: i

* Provide the Key generated from the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it
here: CDAxIGxpbnX4MSAxOTIuMTY4LjAuMzIgOWM5MENlYzNXXXYYYZZZZZ==

Agent information:
ID:001
Name:linux1
IP Address:192.168.2.32

Confirm adding it?(y/n): y

Added.
** Press ENTER to continue.

****************************************
* OSSEC HIDS v0.8 Agent manager. *
* The following options are available: *
****************************************
(I)mport key for the server (I).
(Q)uit.
Choose your actions: I or Q: q

manage_agents: Exiting ..
```

2. After that the agent installation is complete, you can start the OSSEC HIDS service by running the following command:

```
# /opt/ossec/bin/ossec-control start
```